REMARKS

With this Response, Applicants respectfully request that claims 1-27 be canceled without prejudice. Applicants present herein new claims 28-47. Therefore, claims 28-47 are pending.

Objections to the Drawings

The drawings were objected to in the Office Action as failing to comply with 37 C.F.R. §1.84(p)(5) as failing to include reference symbols for 110 and Mi-1 as found in the text of the description. The drawings were also objected to as failing to comply with 37 C.F.R. §1.84 as being informal. Please find submitted concurrently herewith updated formal drawings. Fig. 1 is amended to include a reference symbol 110 and a derived data sequence Mi-1. Applicants also respectfully submit that the drawings filed concurrently herewith are formal drawings complying with 37 C.F.R. § 1.84. Therefore, Applicants respectfully submit that the objections to the drawings have been overcome.

Objection to the Specification

The specification was objected to for various informalities. Specifically, the Description at pages 3 and 11 make reference to a Figure 5, while no Figure 5 was submitted with the application. Applicants have amended the foregoing sections appropriately. Applicants have also amended a paragraph on page 5 to supply missing information. Thus, Applicants respectfully submit that these objections are overcome.

Objection to the Title

The title was objected to as non-descriptive. Please replace the original title "A Dual Use Block/Stream Cipher" with --Combination Block/Stream Cipher Apparatus--. Applicants submit that this title is indicative of the invention as recited in the claims. Independent claim 28 is

directed to an apparatus with a stream cipher key section and a block cipher key section. The remaining pending claims depend from these claims. Independent claim 39 is directed to an apparatus with multiple key sections and a data section. This claim could cover a combination block/stream cipher with a stream cipher key section and a block cipher key section. Therefore, Applicants respectfully request that the objection be withdrawn.

Claim Objections

Claims 23-25 were objected to for informalities. Namely, the claims refer to a first, second, and third register where the parent claim refers to a fourth, fifth, and sixth register. Also, claims 24-25 state "wherein the first plurality...," and should read "wherein the second plurality...." Applicants have elected to cancel these claims; therefore, objection to these claims is moot.

Claim Rejections - 35 U.S.C. § 103

Claims 1-27

Claims 1-2, 4-12, 14-19, and 21-27 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 3,798,360 issued to Feistal (*Feistal*) in view of U.S. Patent No. 4,641,102 issued to Coulthart et al. (*Coulthart*). These claims have been canceled; therefore, rejection of these claims is moot. Claims 3, 13, and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Feistal* and *Coulthart* in view of Schneier, Applied Cryptography, Second Edition, 1996 (*Schneier*). These claims have been canceled; therefore, rejection of these claims is moot.

New Claims 28-47

Applicants present herein claims 28-47. Applicants respectfully submit that these new claims are not rendered obvious by the cited references for at least the following reasons.

Claims 28-38

Claim 28 recites the following:

> **a block cipher key section** to be initialized with a block cipher key, having transformation units to transform the block cipher key;
> a data section coupled with the block cipher key section to be initialized with a random number, having transformation units to transform the random number based on the transformed block cipher key;
> **a stream cipher key section** coupled with the block cipher key section to **modify the block cipher key** according to a stream cipher key to produce data bits to dynamically modify the random number in the data block section; and
> a mapping section to receive the modified random number and the transformed block cipher key and generate a pseudo random bit sequence based on the modified random number and the transformed block cipher key.

Applicants respectfully submit that the cited references fail to disclose or suggest an apparatus comprising a block cipher key section and a stream cipher key section, as recited in claim 28. The Office Action cites *Feistal* as disclosing a first key section and a data section, and states that *Feistal* fails to disclose a second key section. The Office Action cites *Coulthart* as disclosing a key generator, saying the key generator could be the random number generator 43 (RNG) of *Feistal*'s first key section, and equates that with a "second key section." Applicants respectfully submit that even assuming the combination is proper to use *Coulthart*'s key generator as *Feistal*'s RNG, Applicants respectfully submit that the result would be only the single key section of *Feistal*, with the key section using a different RNG than contemplated in *Feistal*. The replacement of one functional block in the key section with a functional block directed to the same function does not convert the single key section into two key sections. Thus, even were the references to be combined as suggested in the Office Action, Applicants respectfully submit that the references fail, either alone or in combination, to disclose or suggest an apparatus comprising a block cipher key section and a stream cipher key section, as claimed.

Because no combination of the references discloses every element of the claims, a prima facie case under MPEP § 2143 is not established under the cited references.

Claims 29-38 depend from claim 28. Because dependent claims necessarily include the limitations of the claims from which they depend, Applicants respectfully submit that these claims are not rendered obvious for at least the reasons set forth above for the independent claims.

Claims 39-47

Claim 39 recites the following:

> **a first key section** to be enabled in a stream cipher mode and disabled in a block cipher mode, and to selectively modify a cipher key;
> **a second key section** to be coupled with the first key section in the stream cipher mode, and **having a first, second, and third registers** to be collectively initialized with the cipher key, and transformation units coupled with the first, second, and third registers to recursively transform the selectively modified cipher key;
> **a data section coupled with the second key section, having a fourth, fifth, and sixth registers** to be collectively initialized with a data bit sequence, and transformation units coupled with the fourth, fifth, and sixth registers to transform the data bit sequence according to the transformed selectively modified cipher key; and
> a mapping section coupled with the second key section and the data section to generate a pseudo random bit sequence with the transformed data bit sequence.

The Office Action at page 5 states that *Feistal* fails to disclose a key section as claimed having a first, second, and third register. The Office Action cites *Coulthart*'s key generator as having a first, second, and third register. The Office Action further cites *Schneier* as supporting the assertion that an XOR function is a substitution, to support the interpretation that *Coulthart*'s XOR units are substitution units. Applicants respectfully submit that even assuming the combination of *Coulthart* with *Feistal* is proper, and the interpretation of *Coulthart* is correct, the result of the combination is at most a single key section having a first, second, and third registers

with substitutions units. The references, either alone or in combination, fail to disclose or suggest an apparatus comprising a first key section coupled with a second key section in a stream cipher mode, as recited in the claim. Because no combination of the references discloses or suggests every element of the claim, Applicants respectfully submit that a proper prima facie obviousness rejection of the claim under MPEP § 2143 is not established with the references.

Claims 40-47 depend from claim 39. Because dependent claims necessarily include the limitations of the claims from which they depend, Applicants respectfully submit that these claims are not rendered obvious by the cited references for at least the reasons set forth above with respect to the independent claim.

Conclusion

Applicants respectfully submit that all rejections have been overcome herein. Therefore, all pending claims are in condition for allowance, and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application.

Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: 2/27/09

Gregory D. Caldwell
Reg. No. 39,926

12400 Wilshire Blvd., 7th Floor
Los Angeles, CA 90025-1026
Telephone: (503) 684-6200

GDC/VHA